

日 本 国 特 許 庁
JAPAN PATENT OFFICE

02.12.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 1 1 月 2 5 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 3 9 4 7 0 9
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 3 9 4 7 0 9]

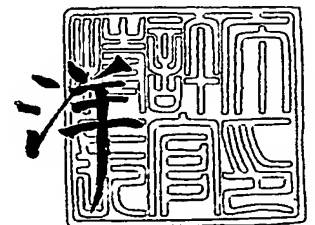
出 願 人 松 下 電 器 産 業 株 式 会 社
Applicant(s):



2 0 0 5 年 1 月 1 3 日

特 許 庁 長 官
Commissioner,
Japan Patent Office

小 川



【書類名】 特許願
【整理番号】 2048150053
【提出日】 平成15年11月25日
【あて先】 特許庁長官 殿
【国際特許分類】 G09C 1/00
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 中野 稔久
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 館林 誠
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 石原 秀志
【特許出願人】
 【識別番号】 000005821
 【氏名又は名称】 松下電器産業株式会社
【代理人】
 【識別番号】 100090446
 【弁理士】
 【氏名又は名称】 中島 司朗
【手数料の表示】
 【予納台帳番号】 014823
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9003742

【書類名】 特許請求の範囲**【請求項 1】**

認証用データの付帯情報を記録する記録媒体と、前記記録媒体から前記付帯情報を読み出す読出装置と、前記記録媒体を利用する端末装置からなる認証システムであって、

前記端末装置は、

複数の認証用データを格納する格納部と、

前記付帯情報を受信する受信部と、

前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部を備え

、比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して複数の認証用データを入手して前記格納部のデータを更新することを特徴とする認証システム。

【請求項 2】

前記複数の認証用データのうち少なくとも 1 つは、前記端末装置自身の有効性を前記読出装置に提示するための認証用データであり、さらに、前記認証用データのうち少なくとも 1 つは、前記読出装置の有効性を検証するための認証用データであることを特徴とする請求項 1 記載の認証システム。

【請求項 3】

前記端末装置はさらに、前記端末装置自身の有効性を前記読出装置に提示するための認証用データから抽出した部分認証用データを前記読出装置へ送信する装置部を備え、

前記読出装置はさらに、前記部分認証用データを受信する受信部を備えることを特徴とする請求項 2 記載の認証システム。

【請求項 4】

前記読出装置はさらに、

認証用データの付帯情報を格納する格納部と、

前記記録媒体から読み出した付帯情報と前記格納する付帯情報を比較する比較部と、

データを送信する送信部を備え、

比較した結果、前記格納する付帯情報が新しいと判断した場合は、前記格納する付帯情報を前記端末装置に送信することを特徴とする請求項 1 記載の認証システム。

【請求項 5】

前記読出装置はさらに、

認証用データを格納する格納部と、

前記記録媒体から読み出した付帯情報と前記格納する認証用データの付帯情報を比較する比較部と、

データを送信する送信部を備え、

比較した結果、前記格納する認証用データの付帯情報が新しいと判断した場合は、前記格納する認証用データを前記端末装置に送信することを特徴とする請求項 1 記載の認証システム。

【請求項 6】

前記記録媒体が、認証用データ自身も記録することを特徴とする請求項 1 記載の認証システム。

【請求項 7】

前記記録媒体の代わりに通信媒体を利用することを特徴とする請求項 1 記載の認証システム。

【請求項 8】

認証用データの付帯情報を記録する記録媒体と、前記記録媒体から前記付帯情報を読み出す読出装置と、前記記録媒体を利用する端末装置からなる認証システムであって、

前記端末装置は、

1 つの認証用データを格納する格納部と、

前記付帯情報を受信する受信部と、

前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部を備え

、比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して前記認証用データを入手して前記格納部のデータを更新し、

前記認証用データは、前記端末装置自身の有効性を前記読出装置に提示するための認証用データであり、さらに、前記認証用データは、前記読出装置の有効性を検証するための認証用データも含むことを特徴とする認証システム。

【請求項 9】

前記端末装置はさらに、

前記端末装置自身の有効性を前記読出装置に提示するための認証用データから抽出した部分認証用データを前記読出装置へ送信する装置部を備え、

前記読出装置はさらに、前記部分認証用データを受信する受信部を備えることを特徴とする請求項 8 記載の認証システム。

【請求項 10】

前記読出装置はさらに、

認証用データの付帯情報を格納する格納部と、

前記記録媒体から読み出した付帯情報と前記格納する付帯情報を比較する比較部と、データを送信する送信部を備え、

比較した結果、前記格納する付帯情報が新しいと判断した場合は、前記格納する付帯情報を前記端末装置に送信することを特徴とする請求項 8 記載の認証システム。

【請求項 11】

前記読出装置はさらに、

認証用データを格納する格納部と、

前記記録媒体から読み出した付帯情報と前記格納する認証用データの付帯情報を比較する比較部と、

データを送信する送信部を備え、

比較した結果、前記格納する認証用データの付帯情報が新しいと判断した場合は、前記格納する認証用データを前記端末装置に送信することを特徴とする請求項 8 記載の認証システム。

【請求項 12】

前記記録媒体が、認証用データ自身も記録することを特徴とする請求項 8 記載の認証システム。

【請求項 13】

前記記録媒体の代わりに通信媒体を利用することを特徴とする請求項 8 記載の認証システム。

【請求項 14】

記録媒体を利用する端末装置であって、

複数の認証用データを格納する格納部と、

前記付帯情報を受信する受信部と、

前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部を備え

、比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して複数の認証用データを入手して前記格納部のデータを更新することを特徴とする端末装置。

【請求項 15】

前記複数の認証用データのうち少なくとも 1 つは、前記端末装置自身の有効性を読出装置に提示するための認証用データであり、さらに、前記認証用データのうち少なくとも 1 つは、前記読出装置の有効性を検証するための認証用データであることを特徴とする請求項 14 記載の端末装置。

【請求項 16】

前記端末装置自身の有効性を前記読出装置に提示するための認証用データから抽出した部分認証用データを前記読出装置へ送信する送信部を備えることを特徴とする請求項 15 記載の端末装置。

【請求項 17】

記録媒体を利用する端末装置であって、
1つの認証用データを格納する格納部と、
前記付帯情報を受信する受信部と、
前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部を備え

、
比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して前記認証用データを入手して前記格納部のデータを更新し、

前記認証用データは、前記端末装置自身の有効性を前記読出装置に提示するための認証用データであり、さらに、前記認証用データは、前記読出装置の有効性を検証するための認証用データも含むことを特徴とする端末装置。

【請求項 18】

前記端末装置自身の有効性を前記読出装置に提示するための認証用データから抽出した部分認証用データを前記読出装置へ送信する送信部を備えることを特徴とする請求項 17 記載の端末装置。

【請求項 19】

記録媒体から付帯情報を読み出す読出装置であって、
認証用データを格納する格納部と、
前記付帯情報を受信する受信部と、
前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部と、
比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して認証用データを入手して前記格納部のデータを更新して、さらに、前記認証用データから前記端末装置自身の有効性を前記読出装置に提示するための部分認証用データを抽出して送信する送信部と、
前記端末装置から部分認証用データを受信する受信部と、
前記受信した部分認証用データを検証する検証部を備えることを特徴とする読出装置。

【請求項 20】

前記読出装置はさらに、
認証用データの付帯情報を格納する格納部と、
記録媒体から読み出した付帯情報と前記格納する付帯情報を比較する比較部と、
データを送信する送信部を備え、
比較した結果、前記格納する付帯情報が新しいと判断した場合は、前記格納する付帯情報を前記端末装置に送信することを特徴とする請求項 19 記載の読出装置。

【請求項 21】

前記読出装置はさらに、
認証用データを格納する格納部と、
記録媒体から読み出した付帯情報と前記格納する認証用データの付帯情報を比較する比較部と、
データを送信する送信部を備え、
比較した結果、前記格納する認証用データの付帯情報が新しいと判断した場合は、前記格納する認証用データを前記端末装置に送信することを特徴とする請求項 19 記載の読出装置。

【請求項 22】

認証用データの付帯情報を記録する記録媒体であって、
端末装置は、認証用データを格納する格納部と、前記付帯情報を受信する受信部と、前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部を備え、比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して

認証用データを入手して前記格納部のデータを更新して、さらに、前記認証用データから前記端末装置自身の有効性を前記読出装置に提示するための部分認証用データを抽出して送信する送信部を備え、

前記記録媒体は、前記端末装置により利用されることを特徴とする記録媒体。

【請求項 23】

認証用データであって、

前記認証用データは、端末装置の有効性を示すデータと、読出装置の有効性を示すデータが一体化されていることを特徴とする認証用データ。

【請求項 24】

前記認証用データは、前記端末装置の有効性を示すデータに対しては、定められた範囲ごとに検証用データが付与され、その一部分のみで正当性を検証できることを特徴とする請求項 23 記載の認証用データ。

【請求項 25】

前記認証用データは、前記読出装置の有効性を示すデータに対しては、その全体に対して検証用データが付与されることを特徴とする請求項 23 記載の認証用データ。

【請求項 26】

前記認証用データは、前記読出装置の有効性を示すデータに対しては、定められた範囲ごとに検証用データが付与され、その一部分のみで正当性を検証できることを特徴とする請求項 23 記載の認証用データ。

【請求項 27】

前記認証用データは、その全体に対して検証用データが付与されていることを特徴とする請求項 24 記載の認証用データ。

【請求項 28】

認証用データであって、

前記認証用データは、有効であることを示すデータ、無効であることを示すデータ、有効である区間を示すデータ、無効である区間を示すデータが混在し、少なくとも 2 つ以上の組み合わせにより構成されることを特徴とする認証用データ。

【請求項 29】

前記認証用データは、区間を示すデータの場合、区間であることを示すフラグが存在することを特徴とする請求項 28 記載の認証用データ。

【請求項 30】

前記認証用データは、端末装置の有効性を示すデータに対しては、定められた範囲ごとに検証用データが付与され、その一部分のみで正当性を検証できることを特徴とする請求項 28 記載の認証用データ。

【請求項 31】

前記認証用データは、前記読出装置の有効性を示すデータに対しては、その全体に対して検証用データが付与されることを特徴とする請求項 28 記載の認証用データ。

【請求項 32】

前記認証用データは、前記読出装置の有効性を示すデータに対しては、定められた範囲ごとに検証用データが付与され、その一部分のみで正当性を検証できることを特徴とする請求項 28 記載の認証用データ。

【請求項 33】

前記認証用データは、その全体に対して検証用データが付与されていることを特徴とする請求項 28 記載の認証用データ。

【書類名】明細書

【発明の名称】認証システム、端末装置、読出装置、記録媒体、及び認証用データ

【技術分野】

【0001】

本発明は、公開鍵暗号を利用した認証システムに関するものであり、公開鍵証明書の有効性を判定するためのリストを含む認証システムに関する。

【背景技術】

【0002】

近年、インターネットの急速な広がりにより、インターネットをその通信の基盤とするシステムも増加している。例えば、インターネットを介して物品の売買を行う電子商取引もその1つである。このような、インターネットを通信の基盤とするシステムにおいては、通信相手がシステムの正当な参加者であることを確認することが必須となる。これを認証という。通信相手としては人間が機器を操作している場合や、機器が予め決められた手順で処理を行う場合があるが、以下ではこの両者を含めて機器という。そして通信相手を認証することを機器認証という。なお、機器が正当性、すなわち自分がシステムの正当な参加者であることを示すことを「証明する」といい、相手の正当性を確認することを「検証する」という。認証とは証明と検証の両方を含む言葉とする。

【0003】

また、暗号技術には共通鍵暗号と公開鍵暗号がある。共通鍵暗号は暗号化のための鍵と復号のための鍵が同じ物である。一方、公開鍵暗号は暗号化のための鍵と復号のための鍵が異なるものである。認証を行うには公開鍵暗号を用いる方が望ましい。なぜならば、共通鍵暗号を用いた認証においては、検証者は証明者と同じ秘密を持つので、これ以降、検証者が証明者になりすます危険性がある。いわゆるパスワード方式はこれに該当する。公開鍵暗号を用いた認証においては、証明者は公開鍵暗号の秘密鍵を用いて証明し、検証者はその秘密鍵に対する公開鍵を用いて検証するのであり、公開鍵から秘密鍵は作成できないようになっているので、認証が終わった後で、検証者が証明者になりすますことができないからである。

【0004】

なお、公開鍵暗号技術において、秘密鍵を用いて処理を行うことを署名といい、対応する公開鍵を用いてその署名の正当性を確認することを検証するという。

公開鍵暗号を用いた相手認証処理の例として、第1の機器が第2の機器にチャレンジデータとして乱数データを送信し、続いて、第2の機器がその乱数データに対して自分の秘密鍵で署名を行って第1の機器にレスポンスデータを返信し、最後に、返信されてきた署名文に対して、第1の機器が第2の機器の公開鍵を用いて検証するというものがある。一般に、このような公開鍵暗号を用いた認証においては、公開鍵そのものが当該システム内で有効なものであることが前提となる。

【0005】

このために、当該システムにおいて認証局 (Certification Authority: 以下、CA) と呼ばれる機関から、各機器に対応する正しい公開鍵であることを示す (公開鍵に対する「お墨付き」となる) 「公開鍵証明書」が発行されることが一般的である。公開鍵証明書は、機器の識別名や有効期限と公開鍵を結合したデータに認証局の電子署名が付与されたものであり、これを受け取った機器は、そのデータに対する認証局の電子署名の正しさを確認し、さらに相手機器の識別名や現在の時間からその公開鍵証明書の記載内容を確認した上で、公開鍵の正しさを確認するものである。さらに、発行された公開鍵証明書のうち、システムから排除され、正当ではないとされる機器の公開鍵証明書については、それらが無効化されていることを他の機器に知らせるために、無効化した公開鍵証明書を特定する情報の一覧に対して認証局の電子署名が付与された公開鍵証明書無効化リスト (Certificate Revocation List: 以下、CRL) として発行される。

【0006】

このように、相手機器の公開鍵を用いてその相手機器を認証する際には、その相手機器の公開鍵証明書を手に入れ、入手した公開鍵証明書がCRLに登録されたもの（無効化されたもの）でないことを確認した上で、上述の認証処理を行うことで、不正な相手機器との取引を回避することができる。なお、CRLの形式、実現例等は、公知の任意の技術で実現可能なため、その詳細についてはここでは言及しない。そのCRLの実現例の一つとしては、特許文献1が開示されており、CRL形式の一例としては、非特許文献1にISO/IEC/ITUが定めたX.509標準で定義されるCRL形式（データ構造）が開示されている。

【特許文献1】特開2003-115838号公報

【特許文献2】特開2002-281013号公報

【非特許文献1】山田慎一郎訳、「デジタル署名と暗号技術」、ピアソン・エデュケーション

【非特許文献2】池野信一、小山謙二、「現代暗号理論」、電子通信学会

【発明の開示】

【発明が解決しようとする課題】

【0007】

しかしながら、前記従来の構成で相手の公開鍵証明書の有効性を判定する場合、当該リストの入手経路の一つとしてネットワーク接続が考えられるが、機器の利用ユーザによりネットワークが遮断されていると、リストが正しく入手／更新されない可能性がある。これは、自身の通信相手が有効か無効かを判断するためだけに用いられるリストに対しては、その入手／更新に対して強制力が働かないためである。

【0008】

本発明は、前記従来の課題を解決するもので、リストのアップデートを強制化可能な認証システムの提供を目的とする。

【課題を解決するための手段】

【0009】

本発明は、認証用データの付帯情報を記録する記録媒体と、前記記録媒体から前記付帯情報を読み出す読出装置と、前記記録媒体を利用する端末装置からなる認証システムであって、前記端末装置は、複数の認証用データを格納する格納部と、前記付帯情報を受信する受信部と、前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部を備え、比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して複数の認証用データを入手して前記格納部のデータを更新することを特徴とする。

【0010】

また、本発明は、前記認証システムであって、前記複数の認証用データのうち少なくとも1つは、前記端末装置自身の有効性を前記読出装置に提示するための認証用データであり、さらに、前記認証用データのうち少なくとも1つは、前記読出装置の有効性を検証するための認証用データであることを特徴とする。

また、本発明は、前記認証システムであって、前記端末装置は、前記端末装置自身の有効性を前記読出装置に提示するための認証用データから抽出した部分認証用データを前記読出装置へ送信する装置部を備え、前記読出装置は、前記部分認証用データを受信する受信部を備えることを特徴とする。

【0011】

また、本発明は、前記認証システムであって、前記読出装置は、認証用データの付帯情報を格納する格納部と、前記記録媒体から読み出した付帯情報と前記格納する付帯情報を比較する比較部と、データを送信する送信部を備え、比較した結果、前記格納する付帯情報が新しいと判断した場合は、前記格納する付帯情報を前記端末装置に送信することを特徴とする。

【0012】

また、本発明は、前記認証システムであって、前記読出装置は、認証用データを格納す

る格納部と、前記記録媒体から読み出した付帯情報と前記格納する認証用データの付帯情報を比較する比較部と、データを送信する送信部を備え、比較した結果、前記格納する認証用データの付帯情報が新しいと判断した場合は、前記格納する認証用データを前記端末装置に送信することを特徴とする。

【0013】

また、本発明は、前記認証システムであって、前記記録媒体が、認証用データ自身も記録することを特徴とする。

また、本発明は、前記認証システムであって、前記記録媒体の代わりに通信媒体を利用することを特徴とする。

また、本発明は、認証用データの付帯情報を記録する記録媒体と、前記記録媒体から前記付帯情報を読み出す読出装置と、前記記録媒体を利用する端末装置からなる認証システムであって、前記端末装置は、1つの認証用データを格納する格納部と、前記付帯情報を受信する受信部と、前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部を備え、比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して前記認証用データを入手して前記格納部のデータを更新し、前記認証用データは、前記端末装置自身の有効性を前記読出装置に提示するための認証用データであり、さらに、前記認証用データは、前記読出装置の有効性を検証するための認証用データも含むことを特徴とする。

【0014】

また、本発明は、前記認証システムであって、前記端末装置は、前記端末装置自身の有効性を前記読出装置に提示するための認証用データから抽出した部分認証用データを前記読出装置へ送信する装置部を備え、前記読出装置は、前記部分認証用データを受信する受信部を備えることを特徴とする。

また、本発明は、前記認証システムであって、前記読出装置は、認証用データの付帯情報を格納する格納部と、前記記録媒体から読み出した付帯情報と前記格納する付帯情報を比較する比較部と、データを送信する送信部を備え、比較した結果、前記格納する付帯情報が新しいと判断した場合は、前記格納する付帯情報を前記端末装置に送信することを特徴とする。

【0015】

また、本発明は、前記認証システムであって、前記読出装置は、認証用データを格納する格納部と、前記記録媒体から読み出した付帯情報と前記格納する認証用データの付帯情報を比較する比較部と、データを送信する送信部を備え、比較した結果、前記格納する認証用データの付帯情報が新しいと判断した場合は、前記格納する認証用データを前記端末装置に送信することを特徴とする。

【0016】

また、本発明は、前記認証システムであって、前記記録媒体が、認証用データ自身も記録することを特徴とする。

また、本発明は、前記認証システムであって、前記記録媒体の代わりに通信媒体を利用することを特徴とする。

また、本発明は、記録媒体を利用する端末装置であって、前記端末装置は、複数の認証用データを格納する格納部と、前記付帯情報を受信する受信部と、前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部を備え、比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して複数の認証用データを入手して前記格納部のデータを更新することを特徴とする。

【0017】

また、本発明は、前記端末装置であって、前記複数の認証用データのうち少なくとも1つは、前記端末装置自身の有効性を読出装置に提示するための認証用データであり、さらに、前記認証用データのうち少なくとも1つは、前記読出装置の有効性を検証するための認証用データであることを特徴とする。

また、本発明は、前記端末装置であって、前記端末装置自身の有効性を前記読出装置に

提示するための認証用データから抽出した部分認証用データを前記読出装置へ送信する送信部を備えることを特徴とする。

【0018】

また、本発明は、記録媒体を利用する端末装置であって、前記端末装置は、1つの認証用データを格納する格納部と、前記付帯情報を受信する受信部と、前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部を備え、比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して前記認証用データを入手して前記格納部のデータを更新し、前記認証用データは、前記端末装置自身の有効性を前記読出装置に提示するための認証用データであり、さらに、前記認証用データは、前記読出装置の有効性を検証するための認証用データも含むことを特徴とする。

【0019】

また、本発明は、前記端末装置であって、前記端末装置自身の有効性を前記読出装置に提示するための認証用データから抽出した部分認証用データを前記読出装置へ送信する送信部を備えることを特徴とする。

また、本発明は、記録媒体から付帯情報を読み出す読出装置であって、端末装置は、認証用データを格納する格納部と、前記付帯情報を受信する受信部と、前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部を備え、比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して認証用データを入手して前記格納部のデータを更新して、さらに、前記認証用データから前記端末装置自身の有効性を前記読出装置に提示するための部分認証用データを抽出して送信する送信部を備え、前記読出装置は、前記端末装置から部分認証用データを受信する受信部と、前記受信した部分認証用データを検証する検証部を備えることを特徴とする。

【0020】

また、本発明は、前記読出装置であって、前記読出装置は、認証用データの付帯情報を格納する格納部と、記録媒体から読み出した付帯情報と前記格納する付帯情報を比較する比較部と、データを送信する送信部を備え、比較した結果、前記格納する付帯情報が新しいと判断した場合は、前記格納する付帯情報を前記端末装置に送信することを特徴とする。

。

【0021】

また、本発明は、前記読出装置であって、前記読出装置は、認証用データを格納する格納部と、記録媒体から読み出した付帯情報と前記格納する認証用データの付帯情報を比較する比較部と、データを送信する送信部を備え、比較した結果、前記格納する認証用データの付帯情報が新しいと判断した場合は、前記格納する認証用データを前記端末装置に送信することを特徴とする。

【0022】

また、本発明は、認証用データの付帯情報を記録する記録媒体であって、端末装置は、認証用データを格納する格納部と、前記付帯情報を受信する受信部と、前記受信した付帯情報と前記格納する認証用データの付帯情報を比較する比較部を備え、比較した結果、前記格納する認証用データの更新が必要と判断した場合は、外部と接続して認証用データを入手して前記格納部のデータを更新して、さらに、前記認証用データから前記端末装置自身の有効性を前記読出装置に提示するための部分認証用データを抽出して送信する送信部を備え、前記記録媒体は、前記端末装置により利用されることを特徴とする。

【0023】

また、本発明は、認証用データであって、前記認証用データは、端末装置の有効性を示すデータと、読出装置の有効性を示すデータが一体化されていることを特徴とする。

また、本発明は、前記認証用データであって、前記認証用データは、前記端末装置の有効性を示すデータに対しては、定められた範囲ごとに検証用データが付与され、その一部分のみで正当性を検証できることを特徴とする。

【0024】

また、本発明は、前記認証用データであって、前記認証用データは、前記読出装置の有

効性を示すデータに対しては、その全体に対して検証用データが付与されることを特徴とする。

また、本発明は、前記認証用データであって、前記認証用データは、前記読出装置の有効性を示すデータに対しては、定められた範囲ごとに検証用データが付与され、その一部分のみで正当性を検証できることを特徴とする。

【0025】

また、本発明は、前記認証用データであって、前記認証用データは、その全体に対して検証用データが付与されていることを特徴とする。

また、本発明は、認証用データであって、前記認証用データは、有効であることを示すデータ、無効であることを示すデータ、有効である区間を示すデータ、無効である区間を示すデータが混在し、少なくとも2つ以上の組み合わせにより構成されることを特徴とする。

。

【0026】

また、本発明は、前記認証用データであって、前記認証用データは、区間を示すデータの場合、区間であることを示すフラグが存在することを特徴とする。

また、本発明は、前記認証用データであって、前記認証用データは、端末装置の有効性を示すデータに対しては、定められた範囲ごとに検証用データが付与され、その一部分のみで正当性を検証できることを特徴とする。

【0027】

また、本発明は、前記認証用データであって、前記認証用データは、前記読出装置の有効性を示すデータに対しては、その全体に対して検証用データが付与されることを特徴とする。

また、本発明は、前記認証用データであって、前記認証用データは、前記読出装置の有効性を示すデータに対しては、定められた範囲ごとに検証用データが付与され、その一部分のみで正当性を検証できることを特徴とする。

【0028】

また、本発明は、前記認証用データであって、前記認証用データは、その全体に対して検証用データが付与されていることを特徴とする。

【発明の効果】

【0029】

本発明によれば、再生装置が、自身が有効であることを示すリストを更新する際に、通信相手の読出装置が有効か無効か判断するためのリストも合わせて更新することで、再生装置における読出装置に関するリストの更新を強制化させることができる。これは、再生装置が、自身が有効であることを示すリストを更新しない場合、読出装置からのコンテンツの供給がストップされることから、再生装置によるリストの更新は必須となり、その更新と合わせて読出装置のリストを更新することにより実現できる。

【0030】

また、本発明によれば、再生装置が、自身の有効性を示すリストと、通信相手である読出装置の有効性を判断するためのリストを保持することから、これら2つのリストを1つにして、自身の有効性を示すリストの更新が、通信相手の有効性を判断するリストの更新と等価になるようにすることでリストの更新を強制化することができる。

【発明を実施するための最良の形態】

【0031】

以下、本発明の実施の形態について、図面を参照しながら説明する。図1は、本発明に係る認証システムの全体構成を示すブロック図である。このシステムは、公開鍵の正当性を示す公開鍵証明書と、読出装置が保持する公開鍵証明書の有効性を示すリスト（以下、リストD）と、再生装置が保持する公開鍵証明書の有効性を示すリスト（以下、リストH）を発行する公開鍵証明書認証局（以下、CA）の端末装置101と、暗号化されたコンテンツ（以下、暗号化コンテンツ）を記録する記録媒体102と、前記記録媒体102から暗号化コンテンツを読み出す読出装置103と、前記読出装置103と認証を行い、前

記暗号化コンテンツを復号して再生する再生装置 104 からなる。

【0032】

ここでは、読出装置の処理負荷を軽減することを目的として、再生装置がリスト D を検索して、通信相手である読出装置が保持する公開鍵証明書が有効か否かを判断し、さらに、同じく再生装置がリスト H を検索して、通信相手である読出装置に対して、自身が保持する公開鍵証明書が有効であることを示すリスト H の部分データを送信する形態とする。このような構成にすることで、読出装置は、再生装置から送られるリスト H の部分データのみを検証/確認するだけで再生装置の有効性を判断することが可能となるため処理負荷の軽減につながる。

【0033】

さらに、再生装置 104 は、自身の有効性を示すリスト H の更新が必要な場合、ネットワークを介して認証局端末装置 101 に接続して、認証局端末装置 101 から更新版のリスト H を取得する。その時、リスト D も同様に取得する。

また、読出装置 103 と再生装置 104 は、汎用の通信路で接続されており、一方が他方を認証する片方向認証、あるいは両者が互いに認証し合う相互認証を実施した後、認証結果が OK であれば、読出装置 103 は、暗号化コンテンツを再生装置 104 へ送信し、再生装置 104 がコンテンツの再生を行う。ここで、汎用の通信路とは、その仕様が公開されているため、通信路上のデータ盗聴、改ざん、差し替えなどの危険に晒される安全でない通信路のことである。

【0034】

次に、図 2、及び図 3 に、読出装置の有効性を判断するためのリスト D の構成、並びに再生装置の有効性を判断するためのリスト H の構成の一例を示す。

図 2 は、読出装置が保持する公開鍵証明書のうち、ID=1、ID=6、ID=7、ID=15 の 4 つの公開鍵証明書が無効化されている場合のリスト D の例を示している。リスト D は、当該リストのバージョン番号を格納するバージョン番号フィールド 201 と、無効化すべき公開鍵証明書の ID を格納する無効化 ID フィールド 202 と、前記フィールドの正当性を検証するための署名を格納する署名フィールド 203 により構成される。図 2 の例では、バージョン番号フィールド 201 には、バージョン番号「0003」が格納され、無効化 ID フィールド 202 には、無効化すべき ID「0001」、「0006」、「0007」、「0015」が格納され、署名フィールド 203 には、前記フィールドの各データが正しいことを示す署名（全フィールドのデータを連結した値に対して CA が付与した署名）が格納される。ただし、記号「||」は、データを連結することを意味する記号として用い、関数 $Sig(X, Y)$ は、データ Y に対して、鍵データ X を用いて署名生成を行う関数として用いる。また、SK_CA は CA だけが保持する署名生成に利用する秘密鍵のことである。

【0035】

なお、前記署名は、必ずしもデータの連結値そのものに署名を付与する必要はなく、データのハッシュ値に署名を付与する形態であってもよい。さらに、前記署名は、付録型の署名である必要はなく、署名検証実施後、署名対象データが生成される回復型の署名であってもよい。その場合、リストには無効化 ID フィールドがなく、検証時に署名から無効化 ID を生成する形態であってもよい。

【0036】

図 3 は、再生装置が保持する公開鍵証明書のうち、ID=1、ID=5、ID=9、ID=13~16 の 7 つの公開鍵証明書が無効化されている場合のリスト H の例を示している。リスト H は、当該リストのバージョン番号を格納するバージョン番号フィールド 301 と、有効な公開鍵証明書の区間の先頭 ID と終端 ID を格納する有効 ID フィールド 302~309 と、前記区間のそれぞれの正当性を検証するための署名を格納する署名フィールド 310~313 により構成される。図 3 の例では、バージョン番号フィールド 301 には、バージョン番号「0003」が格納され、有効 ID フィールド 302~309 には、有効な ID の先頭、及び終端「0002」、「0004」、「0006」、「000

8」、「0010」、「0012」、「0017」、「9999」が格納され、署名フィールド310～313には、前記IDフィールドの区間が正しいことを示す署名（各区間の先頭、及び終端IDに対してCAが付与した署名）が格納される。

【0037】

なお、前記署名は、必ずしもデータの連結値そのものに署名を付与する必要はなく、データのハッシュ値に署名を付与する形態であってもよい。さらに、前記署名は、付録型の署名である必要はなく、署名検証実施後、署名対象データが生成される回復型の署名であってもよい。その場合、リストには有効IDフィールドがなく、検証時に署名から有効IDの先頭、及び終端を生成する形態であってもよい。

【0038】

（実施の形態1）

図4は、本発明の実施の形態1における、読出装置400と再生装置420が相互認証を実行する場合の読出装置400、並びに再生装置420の機能を示す機能ブロック図である。

読出装置400は、CAの公開鍵を格納するCA公開鍵格納部401と、前記CAの公開鍵を用いて、再生装置420から受信した部分リスト、及び証明書に対してCAが付与した署名の正当性を検証する、並びに受信した部分リストと証明書から当該証明書が有効であるか否かを検証する検証部402と、自身の証明書を格納する証明書格納部403と、前記自身の証明書を再生装置420へ送信する証明書送信部404と、読出装置400と再生装置420を接続する汎用通信路上で情報を安全に送信するための認証付き通信路（Secure Authentication Channel：SAC）を確立するのに必要な認証／鍵共有処理を実行する公開鍵暗号処理部405と、記録媒体450に記録されている暗号化コンテンツ鍵を前記処理で共有した鍵（セッション鍵）で暗号化する暗号化部406を備える。

【0039】

また、再生装置420は、自身の証明書を格納する証明書格納部421と、自身の証明書の有効性を示すリストHの最新版を格納する最新リスト格納部422と、前記読出装置400を経由して記録媒体450に記録されているリストD、かつリストHのバージョン番号を受信して、前記最新リスト格納部422に格納するリストHのバージョン番号と新旧を比較し、前記最新リスト格納部に格納するリストHが古い場合に、外部ネットワークとの接続を促し、外部から最新版のリストHを入手して、前記最新リスト格納部に格納するリストHを更新する比較／更新部423と、前記証明書格納部421に格納する証明書と、前記最新リスト格納部422に格納するリストHから、該当するIDの区間、バージョン番号、それらに対する署名からなる部分リストを抽出して、抽出した部分リストと証明書を読出装置400へ送信する証明書／部分リスト送信部424と、CAの公開鍵を格納するCA公開鍵格納部425と、読出装置400の有効性を示すリストDの最新版を格納する最新リスト格納部426と、前記CAの公開鍵を用いて、読出装置400から受信した証明書に対してCAが付与した署名の正当性を検証する、並びに受信した証明書と前記最新リスト格納部426に格納する最新版のリストDから当該証明書が有効であるか否かを検証する検証部427と、再生装置420と読出装置400を接続する汎用通信路上で情報を安全に送信するための認証付き通信路（Secure Authentication Channel：SAC）を確立するのに必要な認証／鍵共有処理を実行する公開鍵暗号処理部428と、読出装置400から受信した2重暗号化されたコンテンツ鍵を前記処理で共有した鍵（セッション鍵）で復号する復号部429と、再生装置420が保持するデバイス鍵を格納するデバイス鍵格納部430と、読出装置400を経由して記録媒体450に記録されている暗号化メディア鍵を受信して、前記デバイス鍵を用いて復号する復号部431と、前記復号して得た暗号化コンテンツ鍵を、同じく前記復号して得たメディア鍵で復号する復号部432と、読出装置400を経由して記録媒体450に記録されている暗号化コンテンツを受信して、前記コンテンツ鍵で復号してコンテンツを獲得する復号部433を備える。

【0040】

また、記録媒体 450 には、暗号化メディア鍵 451、リスト D、かつリスト H のバージョン番号 452、暗号化コンテンツ鍵 453、暗号化コンテンツ 454 が記録されている。

なお、ある特定の装置にだけメディア鍵を与える方法は、公知の任意の技術で実現可能なため、その詳細についてはここでは言及しない。その一例としては、木構造を利用して鍵を管理する特許文献 2 が開示されている。

【0041】

次に、記録媒体 450 に記録される各種データのデータ形式について、図 5 を用いて説明する。

記録媒体 450 は、暗号化メディア鍵を記録する暗号化メディア鍵記録領域 451 と、最新リストのバージョン番号を記録するバージョン番号記録領域 452 と、暗号化コンテンツ鍵を記録する暗号化コンテンツ鍵記録領域 453 と、暗号化コンテンツを記録する暗号化コンテンツ記録領域 454 を備える。

【0042】

最新リストのバージョン番号は、図 5 の例では「0003」である。

暗号化メディア鍵は、ある特定の装置にだけメディア鍵を与えるためのデータであり、メディア鍵を与える装置が持つデバイス鍵 (DK) ではメディア鍵 (Km) を暗号化して、メディア鍵を与えない装置が持つデバイス鍵 (DK) ではメディア鍵とは全く無関係なダミーデータを暗号化する。図 8 は、DK3 を持つ装置と、DK10 を持つ装置に対してはメディア鍵を与えない場合の例を示している。

【0043】

暗号化コンテンツ鍵は、前記メディア鍵で暗号化されたコンテンツ鍵であり、暗号化コンテンツは前記コンテンツ鍵で暗号化されたコンテンツである。

次に、図 6～図 9 を用いて、読出装置 400 と再生装置 420 の動作について説明する。

。 S601: 再生装置 420 は、読出装置 400 を経由して記録媒体 450 からバージョン番号を受信する。

【0044】

S602: 再生装置 420 は、受信したバージョン番号と、自身が保持するリスト H のバージョン番号を比較して、保持するリスト H のバージョン番号が受信したバージョン番号よりも新しいか否かを判断する。

S603: S602 で判断した結果、新しければ S606 へ、古ければ S604 の処理へ移る。

【0045】

S604: 再生装置 420 は、ネットワークを介して外部と接続して、CA から最新のリスト H、並びにリスト D を入手する。

S605: S604 で入手した最新のリストをそれぞれ格納する。

S606: 再生装置 420 は、自身が保持するリスト H と、同じく自身が保持する証明書から該当する部分リストを抽出して、証明書と共に読出装置へ送信する。例えば、証明書 ID として「0007」を持つ再生装置 420 が、図 3 に示すリスト H を保持している場合、自身の有効性を示す 304、305、及び 311 を部分リストとして抽出する。

【0046】

S701: 読出装置 400 は、再生装置 420 から受信した部分リスト、及び証明書に対して、まず、CA の公開鍵を利用してそれぞれに付与されている署名の検証を行う。さらに、部分リストが示す証明書の有効 ID と、受信した再生装置 420 の証明書の ID を比較して、当該証明書が有効か否かを検証する。

S702: S701 で検証した結果、検証結果が全て OK であれば S703 へ、検証結果が 1 つでも NG であれば処理を中止する。

【0047】

S703: 読出装置400は、保持する自身の証明書を再生装置420へ送信する。

S801: 再生装置420は、読出装置400から受信した証明書に対して、まず、CAの公開鍵を利用して付与されている署名の検証を行う。さらに、自身が保持するリストDと、受信した読出装置400の証明書のIDを比較して、当該証明書が有効か否かを検証する。

【0048】

S802: S801で検証した結果、検証結果が全てOKであればS803へ、検証結果が1つでもNGであれば処理を中止する。

S803/S804: 読出装置400と再生装置420の間では、両者の公開鍵暗号化処理部が動作してSACを確立し、データの受け渡しはSACを介して安全に行われる。このSACの実現方法については、後に詳細を述べる。SAC処理の結果として、両者はセッション鍵を共有する。

【0049】

S901: 読出装置400は、S804で生成したセッション鍵を用いて、記録媒体450に記録されている暗号化コンテンツ鍵をさらに暗号化して再生装置420へ送信する。

S902: 再生装置420は、読出装置400から受信した2重暗号化されたコンテンツ鍵を、S803で得たセッション鍵で復号して暗号化コンテンツ鍵を得る。

【0050】

S903: 再生装置420は、読出装置400を経由して記録媒体450から暗号化メディア鍵を受信して、保持するデバイス鍵で復号してメディア鍵を得る。さらに、S902で得た暗号化コンテンツ鍵を前記メディア鍵で復号してコンテンツ鍵を得る。

S904: 再生装置420は、読出装置400を経由して記録媒体450から暗号化コンテンツを受信して、S903で得たコンテンツ鍵で復号してコンテンツを得る。

【0051】

以上に示したように、再生装置の保持するリストHが古い場合、リストHを更新しなければ、再生装置は読出装置によって認証されないため、再生装置のリストHの更新を促す/強制化することができる。その際に、リストDも合わせて更新することにより、本来強制力の働かないリストDの更新も行うことが可能となる。

次に、読出装置400と再生装置420との間で設定されるSACの実現方法について図10を用いて説明する。ただし、 $Sign()$ を署名生成関数、 $Veri()$ を署名検証関数、 $Gen()$ を鍵生成関数とし、 Y をそのシステム固有のシステムパラメータとする。また、鍵生成関数 $Gen()$ は、 $Gen(x, Gen(y, z)) = Gen(y, Gen(x, z))$ の関係を満たすものとする。なお、このような鍵生成関数は、公知の任意の技術で実現可能なため、その詳細についてはここでは言及しない。その一例としては、非特許文献2に、ディフィーヘルマン(DH)型公開鍵配送法が開示されている。

【0052】

S1001: 読出装置Aは、CAが発行した証明書 $Cert_A$ を再生装置Bに送信する。ここでは、証明書の構成要素は、Aの公開鍵 PK_A 、AのID(ID_A)、それらに対するCAの署名 Sig_CA としている。

S1002: 再生装置Bは、CAの公開鍵 P_CA を用いて $Cert_A$ に付与されている署名 Sig_CA が正しいか否かを検証する。検証結果が正しくない場合、SACの設定処理を終了する。さらに、再生装置Bは、読出装置AのID(ID_A)が、CRLに登録されているか否かを確認する。登録されている場合も、SACの設定処理を終了する。

【0053】

S1003: 再生装置Bは、CAが発行した証明書 $Cert_B$ を読出装置Aに送信する。ここでは、証明書の構成要素は、Bの公開鍵 PK_B 、BのID(ID_B)、それらに対するCAの署名 Sig_CA としている。

S1004: 読出装置Aは、CAの公開鍵 P_CA を用いて $Cert_B$ に付与されて

いる署名 Sig_CA が正しいか否かを検証する。検証結果が正しくない場合、SAC の設定処理を終了する。さらに、読出装置 A は、再生装置 B の ID (ID_B) が、CRL に登録されているか否かを確認する。登録されている場合も、SAC の設定処理を終了する。

【0054】

S1005: 読出装置 A は、乱数 Cha_A を生成して、再生装置 B に送信する。

S1006: 再生装置 B は、受信した Cha_A に対して、自身の秘密鍵 SK_B で署名 Sig_B を生成して、読出装置 A に送信する。

S1007: 読出装置 A は、S1003 で受信した再生装置 B の公開鍵 PK_B を用いて、 Sig_B が正しいか否かを検証する。検証結果が正しくない場合、SAC の設定処理を終了する。

【0055】

S1008: 再生装置 B は、乱数 Cha_B を生成して、読出装置 A に送信する。

S1009: 読出装置 A は、受信した Cha_B に対して、自身の秘密鍵 SK_A で署名 Sig_A を生成して、再生装置 B に送信する。

S1010: 再生装置 B は、S1001 で受信した読出装置 A の公開鍵 PK_A を用いて、 Sig_A が正しいか否かを検証する。検証結果が正しくない場合、SAC の設定処理を終了する。

【0056】

S1011: 再生装置 B は、乱数 b を生成し、 $Key_B = Gen(b, Y)$ を計算して読出装置 A に送信する。

S1012: 読出装置 A は、乱数 a を生成し、 $Key_A = Gen(a, Y)$ を計算して再生装置 B に送信する。さらに、読出装置 A は、両者で共有する鍵 $Key_AB = Gen(b, Key_A)$ を算出する。

【0057】

S1013: 再生装置 B は、両者で共有する鍵 $Key_AB = Gen(a, Key_B)$ を算出する。

(実施の形態 2)

図 11 は、本発明の実施の形態 2 における、読出装置 1100 と再生装置 1120 が相互認証を実行する場合の読出装置 1100、並びに再生装置 1120 の機能を示す機能ブロック図である。

【0058】

読出装置 1100 は、CA の公開鍵を格納する CA 公開鍵格納部 1101 と、前記 CA の公開鍵を用いて、再生装置 1120 から受信した部分リスト、及び証明書に対して CA が付与した署名の正当性を検証する、並びに受信した部分リストと証明書から当該証明書が有効であるか否かを検証する検証部 1102 と、自身の証明書を格納する証明書格納部 1103 と、前記自身の証明書を再生装置 1120 へ送信する証明書送信部 1104 と、読出装置 1100 と再生装置 1120 を接続する汎用通信路上で情報を安全に送信するための認証付き通信路 (Secure Authentication Channel: SAC) を確立するのに必要な認証/鍵共有処理を実行する公開鍵暗号処理部 1105 と、記録媒体 1150 に記録されている暗号化コンテンツ鍵を前記処理で共有した鍵 (セッション鍵) で暗号化する暗号化部 1106 を備える。

【0059】

また、再生装置 1120 は、自身の証明書を格納する証明書格納部 1121 と、自身の証明書、並びに読出装置の有効性を示すリストの最新版を格納する最新リスト格納部 1122 と、前記読出装置 1100 を経由して記録媒体 1150 に記録されているリストのバージョン番号を受信して、前記最新リスト格納部 1122 に格納するリストのバージョン番号と新旧を比較し、前記最新リスト格納部に格納するリストが古い場合に、外部ネットワークとの接続を促し、外部から最新版のリストを入手して、前記最新リスト格納部に格納するリストを更新する比較/更新部 1123 と、前記証明書格納部 1121 に格納する

証明書と、前記最新リスト格納部 1122 に格納するリストから、該当する ID の区間、バージョン番号、それらに対する署名からなる部分リストを抽出して、抽出した部分リストと証明書を読出装置 1100 へ送信する証明書／部分リスト送信部 1124 と、CA の公開鍵を格納する CA 公開鍵格納部 1125 と、前記 CA の公開鍵を用いて、読出装置 1100 から受信した証明書に対して CA が付与した署名の正当性を検証する、並びに受信した証明書と前記最新リスト格納部 1126 に格納する最新版のリストから当該証明書が有効であるか否かを検証する検証部 1127 と、再生装置 1120 と読出装置 1100 を接続する汎用通信路上で情報を安全に送信するための認証付き通信路 (Secure Authentication Channel: SAC) を確立するのに必要な認証／鍵共有処理を実行する公開鍵暗号処理部 1128 と、読出装置 1100 から受信した 2 重暗号化されたコンテンツ鍵を前記処理で共有した鍵 (セッション鍵) で復号する復号部 1129 と、再生装置 1120 が保持するデバイス鍵を格納するデバイス鍵格納部 1130 と、読出装置 1100 を経由して記録媒体 1150 に記録されている暗号化メディア鍵を受信して、前記デバイス鍵を用いて復号する復号部 1131 と、前記復号して得た暗号化コンテンツ鍵を、同じく前記復号して得たメディア鍵で復号する復号部 1132 と、読出装置 1100 を経由して記録媒体 1150 に記録されている暗号化コンテンツを受信して、前記コンテンツ鍵で復号してコンテンツを獲得する復号部 1133 を備える。

【0060】

また、記録媒体 1150 には、暗号化メディア鍵 1151、最新リストのバージョン番号 1152、暗号化コンテンツ鍵 1153、暗号化コンテンツ 1154 が記録されている。

なお、ある特定の装置にだけメディア鍵を与える方法は、公知の任意の技術で実現可能なため、その詳細についてはここでは言及しない。その一例としては、木構造を利用して鍵を管理する特許文献 2 が開示されている。

【0061】

次に、図 12 にリストの一例を示す。図 12 は、読出装置が保持する公開鍵証明書のうち、ID=1、ID=2 の 2 つの公開鍵証明書が無効化されている場合、及び再生装置が保持する公開鍵証明書のうち、ID=9、ID=13~16 の 5 つの公開鍵証明書が無効化されている場合のリストの例を示している。リストは、当該リストのバージョン番号を格納するバージョン番号フィールド 1201 と、読出装置の無効化すべき公開鍵証明書の ID を格納する無効化 ID フィールド 1202~1203 と、有効な公開鍵証明書の区間の先頭 ID と終端 ID を格納する有効 ID フィールド 1204~1209 と、前記区間のそれぞれの正当性を検証するための署名を格納する署名フィールド 1210~1212 と、リスト全体の正当性を検証するための署名を格納する署名フィールド 1213 により構成される。図 12 の例では、バージョン番号フィールド 1201 には、バージョン番号「0003」が格納され、無効化 ID フィールド 1202~1203 には、読出装置の無効化すべき ID 「0001」、「0002」が格納され、有効 ID フィールド 1204~1209 には、再生装置の有効な ID の先頭、及び終端「0006」、「0008」、「0010」、「0012」、「0017」、「9999」が格納され、署名フィールド 1210~1212 には、前記有効 ID フィールドの区間が正しいことを示す署名 (各区間の先頭、及び終端 ID に対して CA が付与した署名) が格納され、署名フィールド 1213 には、前記フィールドの各データが正しいことを示す署名 (全フィールドのデータを連結した値に対して CA が付与した署名) が格納される。なお、前記署名は、必ずしもデータの連結値そのものに署名を付与する必要はなく、データのハッシュ値に署名を付与する形態であってもよい。さらに、前記署名は、付録型の署名である必要はなく、署名検証実施後、署名対象データが生成される回復型の署名であってもよい。その場合、リストには無効化 ID フィールドがなく、検証時に署名から無効化 ID を生成する形態であってもよい。

【0062】

次に、図 13~図 16 を用いて、読出装置 1100 と再生装置 1120 の動作について

説明する。

S1301:再生装置1120は、読出装置1100を経由して記録媒体1150からバージョン番号を受信する。

S1302:再生装置1120は、受信したバージョン番号と、自身が保持するリストのバージョン番号を比較して、保持するリストのバージョン番号が受信したバージョン番号よりも新しいか否かを判断する。

【0063】

S1303:S1302で判断した結果、新しいければS1306へ、古ければS1304の処理へ移る。

S1304:再生装置1120は、ネットワークを介して外部と接続して、CAから最新のリストを入手する。

S1305:S1304で入手した最新のリストをそれぞれ格納する。

【0064】

S1306:再生装置1120は、自身が保持するリストと、同じく自身が保持する証明書から該当する部分リストを抽出して、証明書と共に読出装置へ送信する。例えば、証明書IDとして「0007」を持つ再生装置1120が、図12に示すリストを保持している場合、自身の有効性を示す1204、1205、及び1210を部分リストとして抽出する。

【0065】

S1401:読出装置1100は、再生装置1120から受信した部分リスト、及び証明書に対して、まず、CAの公開鍵を利用してそれぞれに付与されている署名の検証を行う。さらに、部分リストが示す証明書の有効IDと、受信した再生装置1120の証明書のIDを比較して、当該証明書が有効か否かを検証する。

S1402:S1401で検証した結果、検証結果が全てOKであればS1403へ、検証結果が1つでもNGであれば処理を中止する。

【0066】

S1403:読出装置1100は、保持する自身の証明書を再生装置1120へ送信する。

S1501:再生装置1120は、読出装置1100から受信した証明書に対して、まず、CAの公開鍵を利用して付与されている署名の検証を行う。さらに、自身が保持するリストと、受信した読出装置1100の証明書のIDを比較して、当該証明書が有効か否かを検証する。

【0067】

S1502:S1501で検証した結果、検証結果が全てOKであればS1503へ、検証結果が1つでもNGであれば処理を中止する。

S1503/S1504:読出装置1100と再生装置1120の間では、両者の公開鍵暗号化処理部が動作してSACを確立し、データの受け渡しはSACを介して安全に行われる。このSACの実現方法については、後に詳細を述べる。SAC処理の結果として、両者はセッション鍵を共有する。

【0068】

S1601:読出装置1100は、S1504で生成したセッション鍵を用いて、記録媒体1150に記録されている暗号化コンテンツ鍵をさらに暗号化して再生装置1120へ送信する。

S1602:再生装置1120は、読出装置1100から受信した2重暗号化されたコンテンツ鍵を、S1503で得たセッション鍵で復号して暗号化コンテンツ鍵を得る。

【0069】

S1603:再生装置1120は、読出装置1100を経由して記録媒体1150から暗号化メディア鍵を受信して、保持するデバイス鍵で復号してメディア鍵を得る。さらに、S1602で得た暗号化コンテンツ鍵を前記メディア鍵で復号してコンテンツ鍵を得る。

。

S1604:再生装置1120は、読出装置1100を経由して記録媒体1150から暗号化コンテンツを受信して、S1603で得たコンテンツ鍵で復号してコンテンツを得る。

【0070】

(その他の変形例)

(1) 本発明の実施の形態1では、無効化するID、及び有効なIDの区間でリストを構成する形態とし、実施の形態2では、無効化するID、及び有効なIDの区間で1つのリストを構成する形態としたが、本発明はその構成に限定されるものではない。例えば、図17に示すように、1つのリスト内に無効化するIDを示すフィールド1702~1703、有効なIDを示すフィールド1704~1705、有効なIDの区間を示すフィールド1706~1707、あるいはそれらの組み合わせでリストを構成する形態であってもよい。

【0071】

さらに、例えば、図18に示すように、無効化するIDを示すフィールド1802~1804、1807に対しては、その先頭にビット「0」を付与し、複数の無効化するID(区間)を示す1805~1806には、その先頭にビット「1」を付与してリストを構成する形態であってもよい。

(2) 本発明の実施の形態1、及び実施の形態2では、記録媒体には予め暗号化されたコンテンツが記録されているDVD-Videoのようなプリレコーディッドメディアの形態としたが、本発明はその構成に限定されるものではない。例えば、DVD-RAMのようなレコーダブルメディアであってもよい。その場合、実施の形態1、及び実施の形態2と同様に認証を実行した後で、暗号化されたコンテンツが記録媒体に記録される形態となる。さらにその場合は、実施の形態1、及び実施の形態2は、再生装置の代わりに記録装置により実現される。

【0072】

(3) 本発明の実施の形態1、及び実施の形態2では、記録媒体にはバージョン番号のみが記録されている形態としたが、本発明はその構成に限定されるものではない。例えば、記録媒体には、バージョン番号と共に、最新リストも記録されており、記録媒体に記録されている最新リストを利用して再生装置がリストを更新する構成であってもよい。

(4) 実施の形態1、及び実施の形態2において、読出装置が、リストのバージョン番号を格納する格納部を有する構成であってもよい。この場合、読出装置は、記録媒体から読み出したバージョン番号と、自身が保持するバージョン番号を比較して、新しいバージョン番号を再生装置に送信する構成であってもよい。

【0073】

さらに、読出装置が、リストのバージョン番号に加え、リスト自身を格納する格納部を有する構成であってもよい。この場合、読出装置は、記録媒体から読み出したバージョン番号と、自身が保持するバージョン番号を比較して、自身が保持するバージョン番号が新しければ、保持するバージョン番号、並びにリストを再生装置に送信する構成であってもよい。

【0074】

(5) 本発明の実施の形態1、及び実施の形態2では、認証に用いるデータ、及びコンテンツが記録媒体に記録される形態としたが、本発明はその構成に限定されるものではない。記録媒体の代わりに通信媒体を利用して、通信媒体を介して、認証に用いるデータ、及びコンテンツを受け渡しする構成であってもよい。また、記録媒体、並びに通信媒体を併用する形態であってもよい。

【0075】

(6) 本発明の実施の形態1、及び実施の形態2では、認証に用いるデータの保護にCAの署名を用いる形態としたが本発明はその構成に限定されるものではない。例えば、読出装置は読出装置専用の秘密鍵を保持し、再生装置は再生装置専用の秘密鍵を用いる構成として、認証に用いるデータには、各秘密鍵を利用して生成された認証子を付与する構成

であってもよい。

【0076】

(7) 実施の形態1、及び実施の形態2において、再生装置が、例えばPCにインストールされる再生用ソフトウェアであってもよい。あるいは、記録用ソフトウェアであってもよい。

【産業上の利用可能性】

【0077】

本発明にかかる認証システムは、更新の強制力が働かない読出装置に対するリストの更新を、再生装置自身のリストの更新と同時に進行、あるいはリスト自身を一体化させることにより、効果的な認証を実現できるという効果を有し、公開鍵暗号を利用した認証システムにおいて有用である。

【図面の簡単な説明】

【0078】

【図1】 本発明に係る認証システムの全体構成を示すブロック図

【図2】 本発明に係るリストの例を示す図

【図3】 本発明に係るリストの例を示す図

【図4】 本発明の実施の形態1における機能ブロック図

【図5】 本発明の実施の形態1における記録媒体に記録されるデータの例を示す図

【図6】 本発明の実施の形態1における動作を示す図

【図7】 本発明の実施の形態1における動作を示す図

【図8】 本発明の実施の形態1における動作を示す図

【図9】 本発明の実施の形態1における動作を示す図

【図10】 本発明に係る相互認証の例を示す図

【図11】 本発明の実施の形態2における機能ブロック図

【図12】 本発明の実施の形態2に係るリストの例を示す図

【図13】 本発明の実施の形態2における動作を示す図

【図14】 本発明の実施の形態2における動作を示す図

【図15】 本発明の実施の形態2における動作を示す図

【図16】 本発明の実施の形態2における動作を示す図

【図17】 本発明に係るリストの例を示す図

【図18】 本発明に係るリストの例を示す図

【符号の説明】

【0079】

101 認証局端末装置

102、450、1150 記録媒体

103、400、1100 読出装置

104、420、1120 再生装置

401、425、1101、1125 CA公開鍵格納部

402、427、1102、1127 検証部

403、421、1103、1121 証明書格納部

404、1104 証明書送信部

405、428、1105、1128 公開鍵暗号処理部

406、1106 暗号化部

422、426、1122、1126 最新リスト格納部

423、1123 比較／更新部

424、1124 証明書／部分リスト送信部

429、431、432、433、1129、1131、1132、1133 復号部

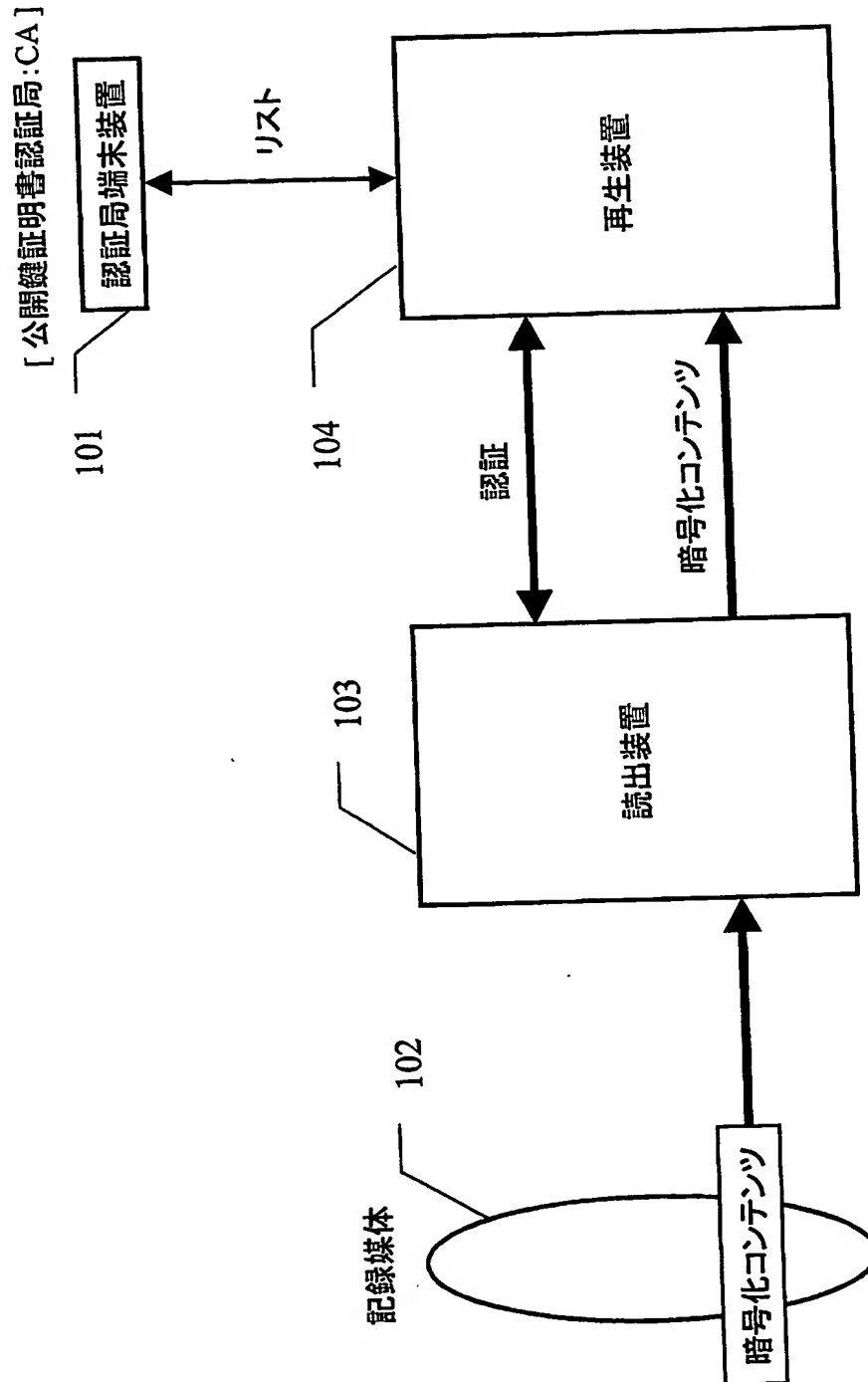
430、1130 デバイス鍵格納部

451、1151 暗号化メディア鍵

452、1152 バージョン番号

4 5 3、1 1 5 3 暗号化コンテンツ鍵
4 5 4、1 1 5 4 暗号化コンテンツ

【書類名】 図面
【図 1】



【図 2】

バージョン番号:VN	0003	202	203
無効化する証明書のID:ID1	0001		
無効化する証明書のID:ID2	0006		
無効化する証明書のID:ID3	0007		
無効化する証明書のID:ID4	0015		
CAの署名	Sig(SK_CA, VN RID1 RID2 RID3 RID4)		

証明書ID : x, 2, 3, 4, 5, x, x, 8, 9, ..., D8, 16, ...

x : 無効化すべきID

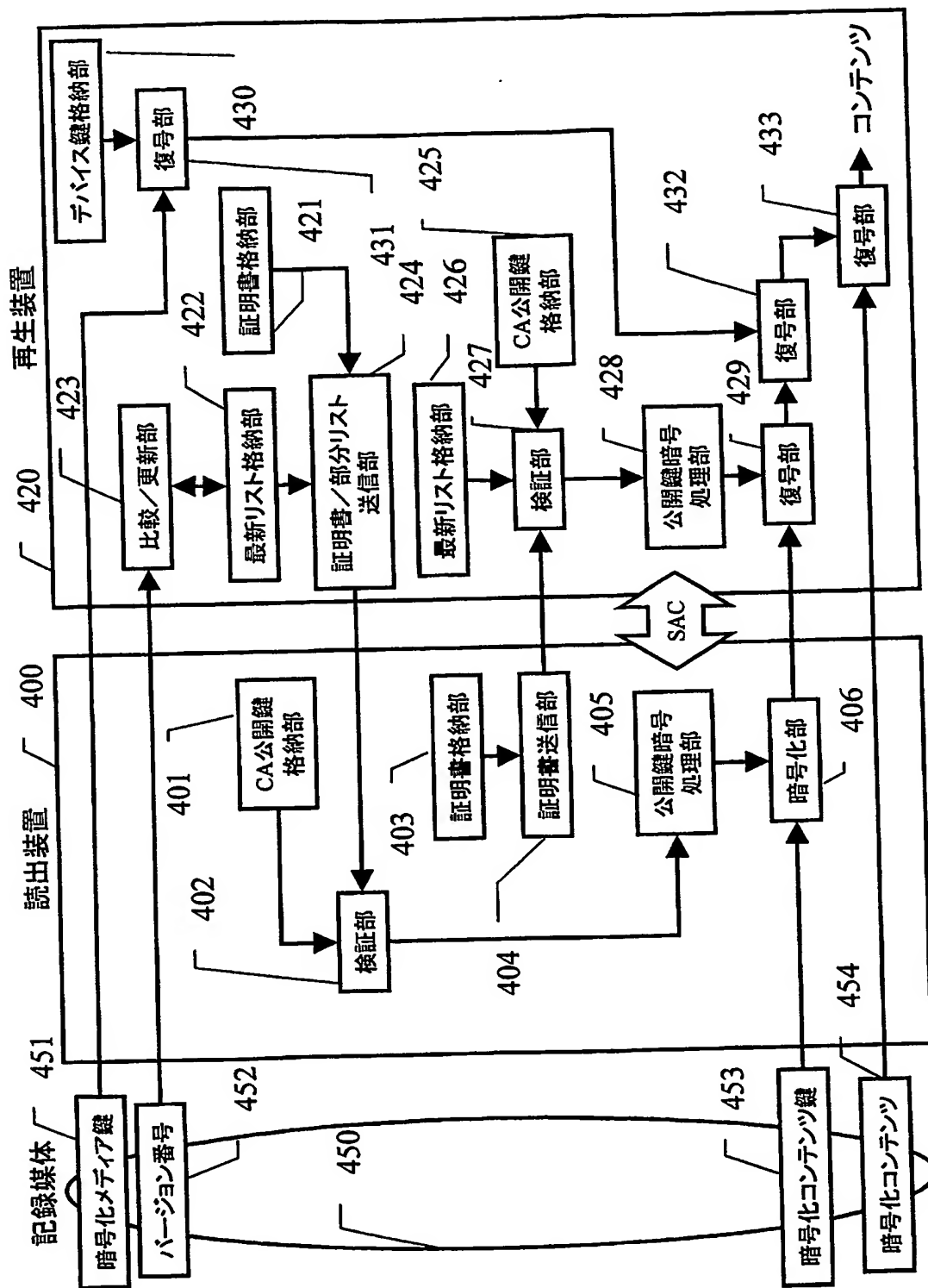
【図 3】

バージョン番号:VN	0003	301
有効な証明書の先頭ID:ID1	0002	302
有効な証明書の終端ID:ID2	0004	303
有効な証明書の先頭ID:ID3	0006	304
有効な証明書の終端ID:ID4	0008	305
有効な証明書の先頭ID:ID5	0010	306
有効な証明書の終端ID:ID6	0012	307
有効な証明書の先頭ID:ID7	0017	308
有効な証明書の終端ID:ID8	9999	309
CAの署名	Sig(SK_CA, VN ID1 ID2)	310
CAの署名	Sig(SK_CA, VN ID3 ID4)	311
CAの署名	Sig(SK_CA, VN ID5 ID6)	312
CAの署名	Sig(SK_CA, VN ID7 ID8)	313

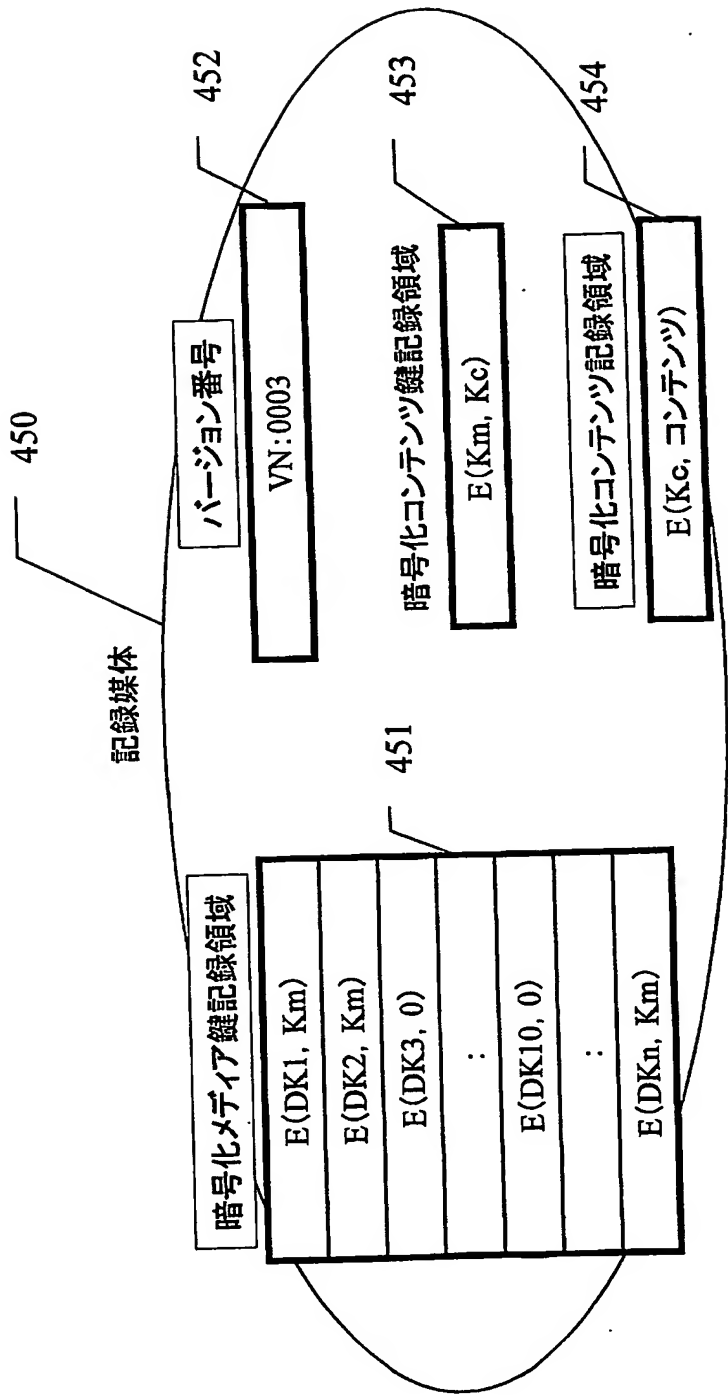
証明書ID : x 2, 3, 4, x 6, 7, 8, x 10, 11, 12, x3, x4, x6, 17, 18, ..., 9999

x : 無効化すべきID

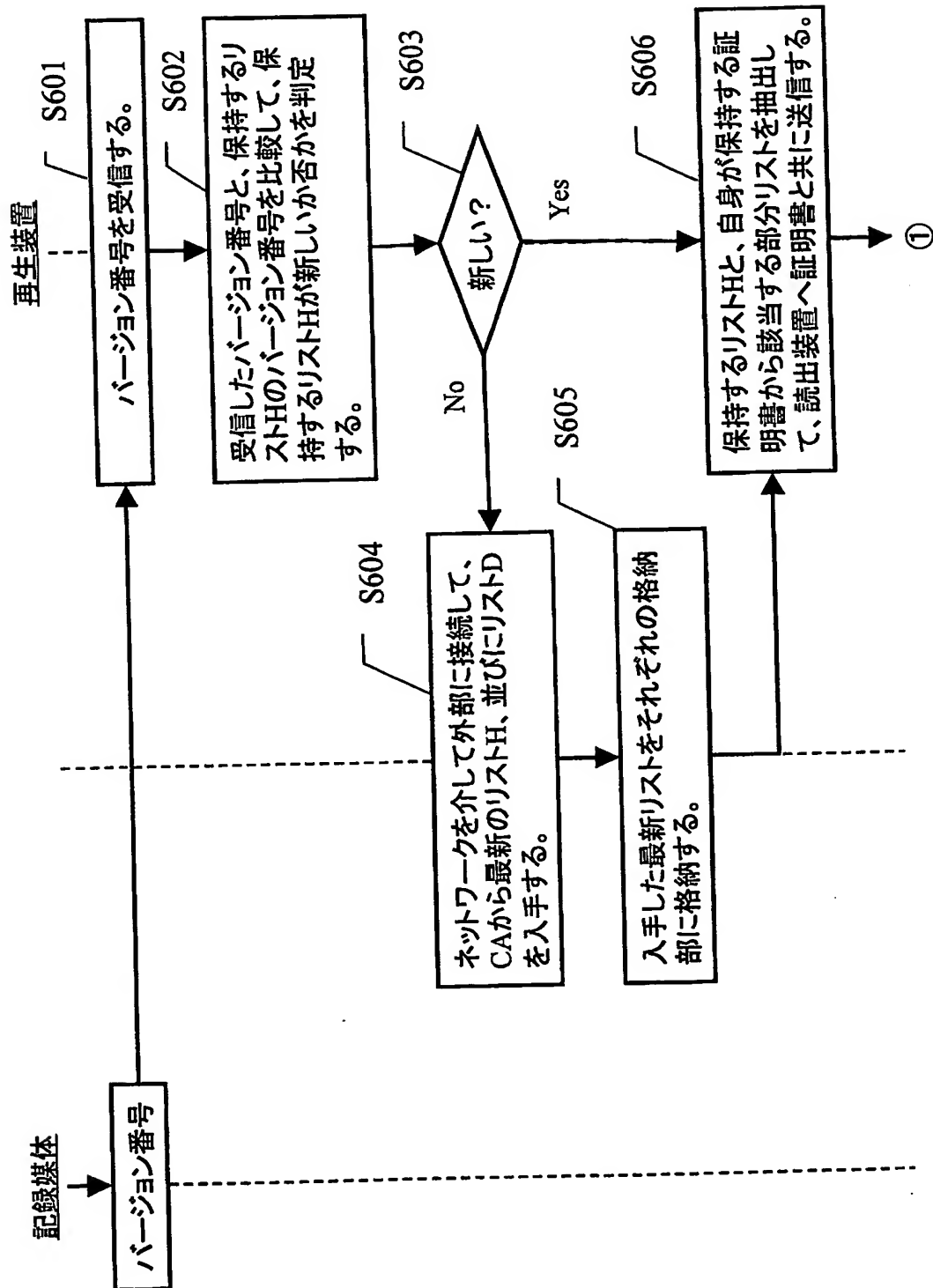
【図4】



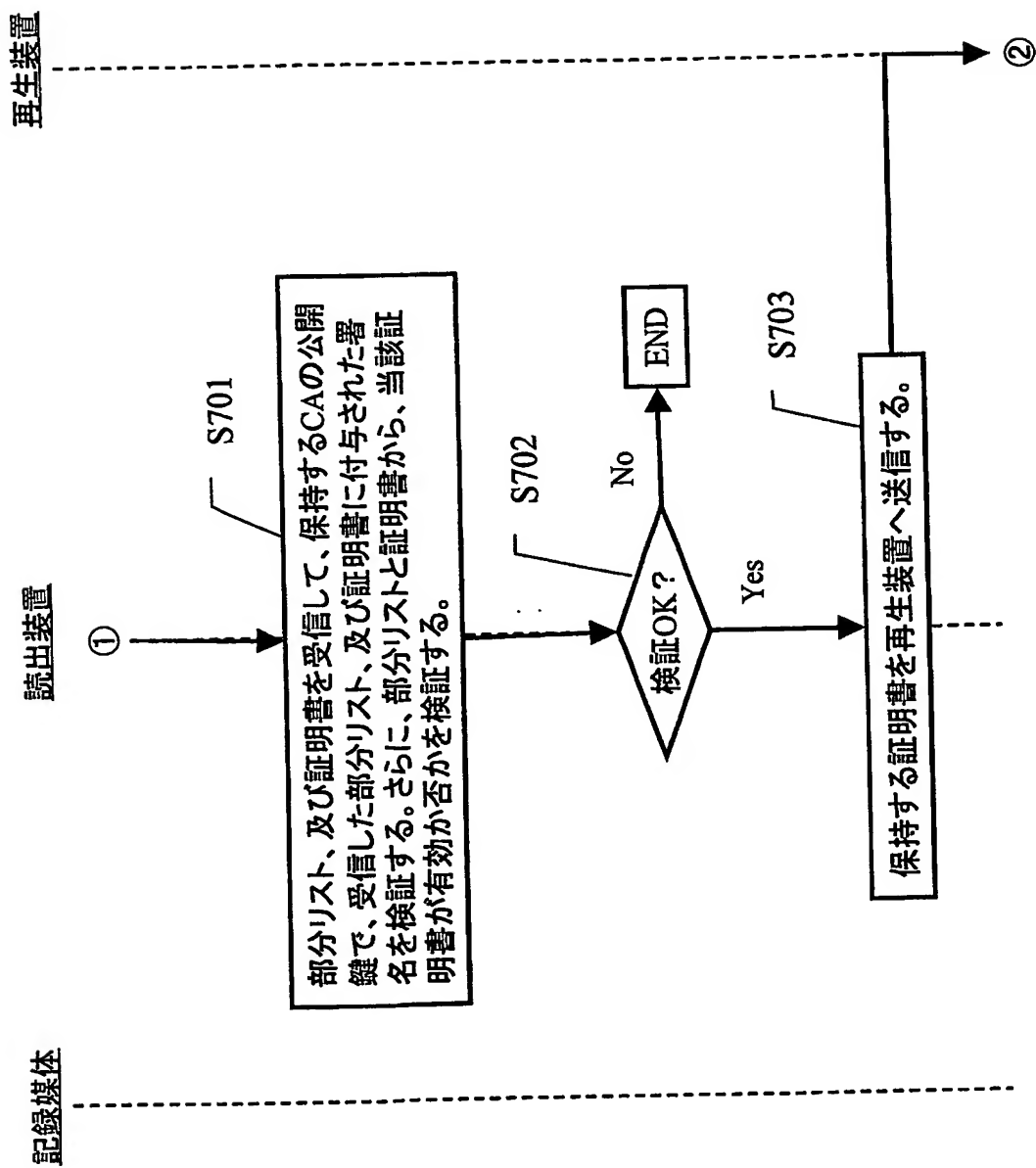
【図 5】



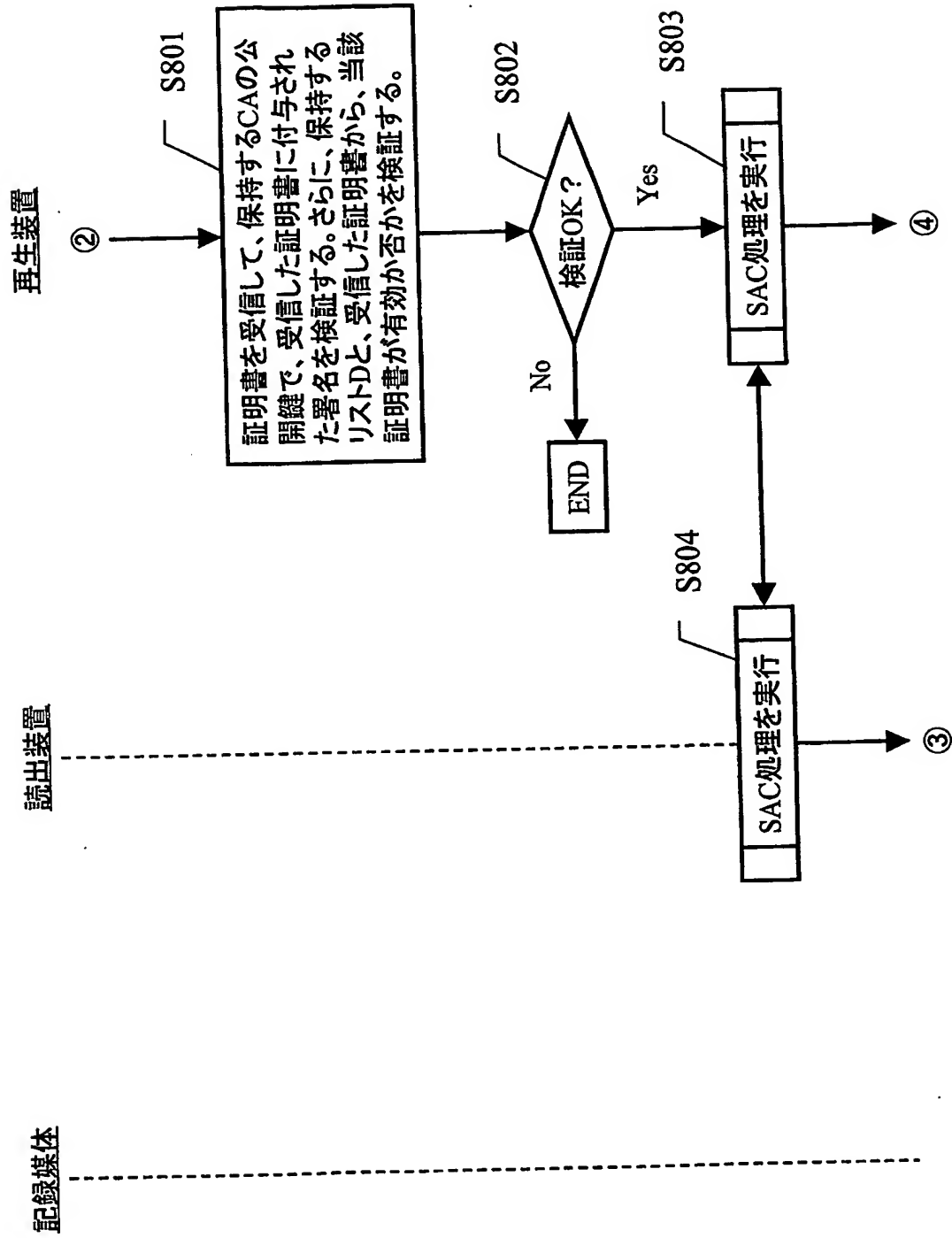
【図 6】



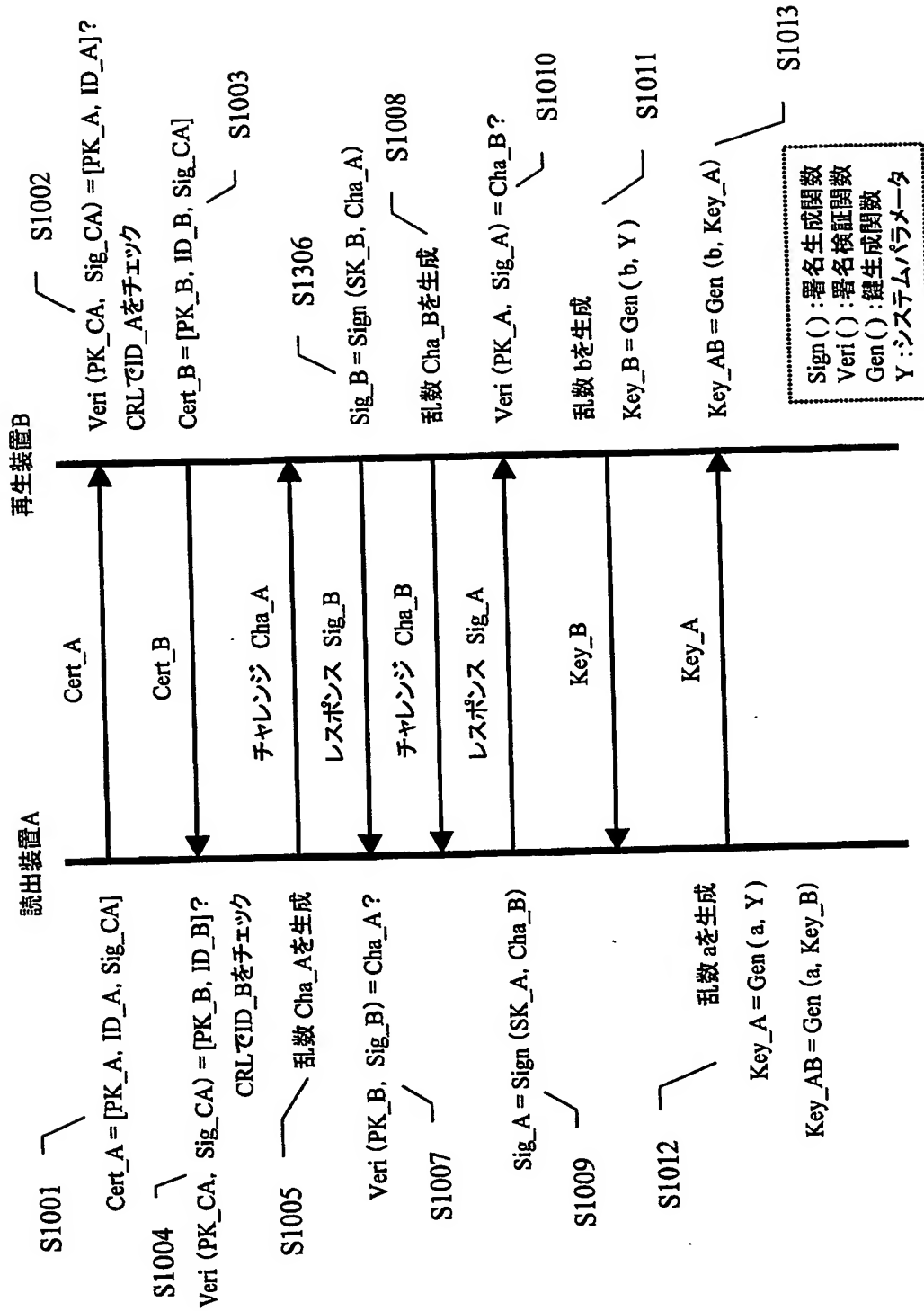
【図 7】



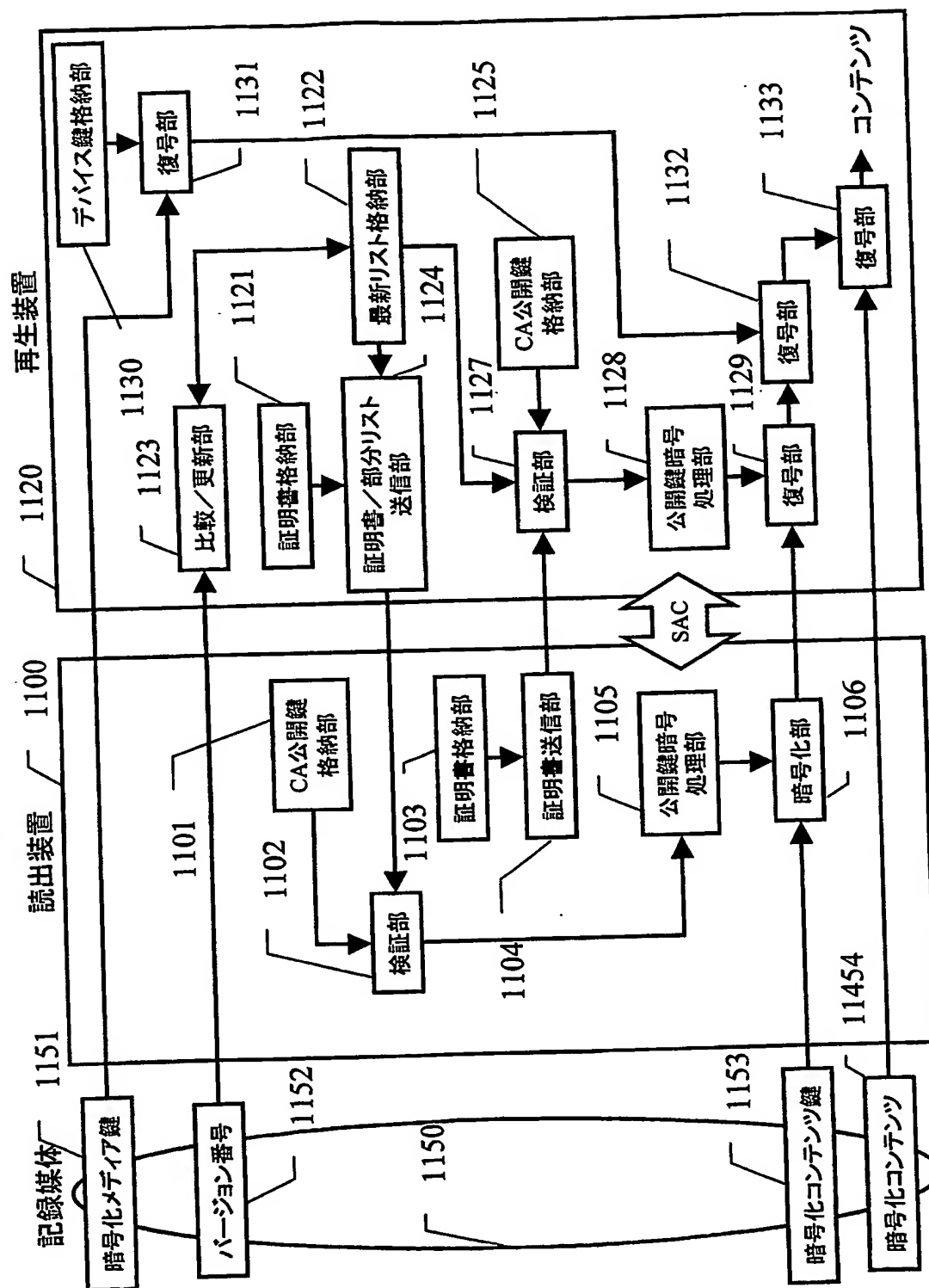
【図 8】



【図 10】



【図 11】



【図 12】

バージョン番号:VN	0003	1201
(読出装置の)無効化するID:ID1	0001	1202
(読出装置の)無効化するID:ID2	0002	1203
(再生装置の)有効な証明書の先頭ID:ID3	0006	1204
(再生装置の)有効な証明書の終端ID:ID4	0008	1205
(再生装置の)有効な証明書の先頭ID:ID5	0010	1206
(再生装置の)有効な証明書の終端ID:ID6	0012	1207
(再生装置の)有効な証明書の先頭ID:ID7	0017	1208
(再生装置の)有効な証明書の終端ID:ID8	9999	1209
CAの署名	Sig1(SK_CA, VN ID3 ID4)	1210
CAの署名	Sig2(SK_CA, VN ID5 ID6)	1211
CAの署名	Sig3(SK_CA, VN ID7 ID8)	1212
CAの署名	Sig(SK_CA, VN ID1 ID2 ID3 ID4 ID5 ID6 ID7 ID8 Sig1 Sig2 Sig3)	1213

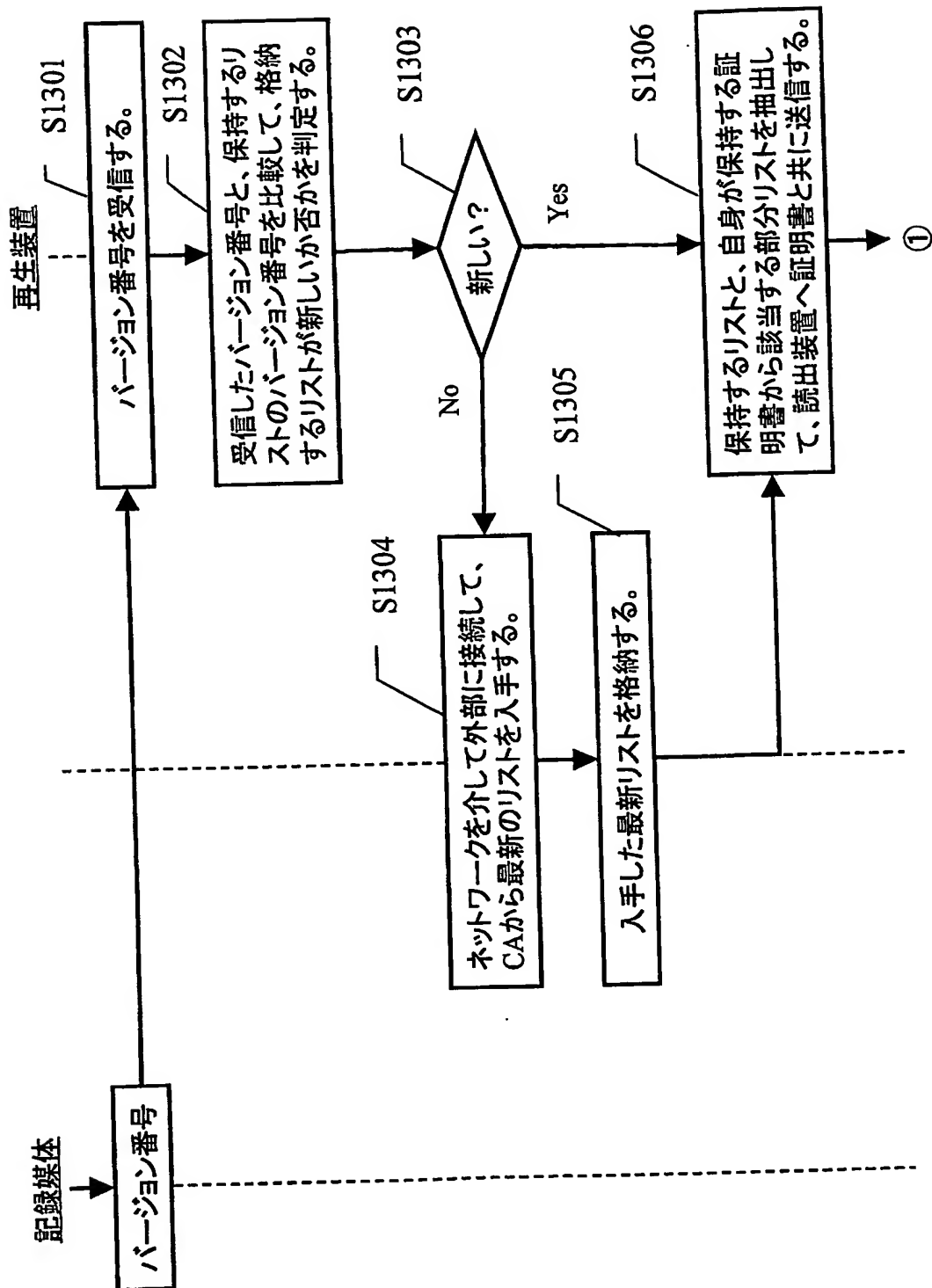
証明書ID : K & 3, 4, 5, 6, 7, 8, 9 10, 11, 12, 13, 14, 15, 16, 17, 18, ...

読出装置のID

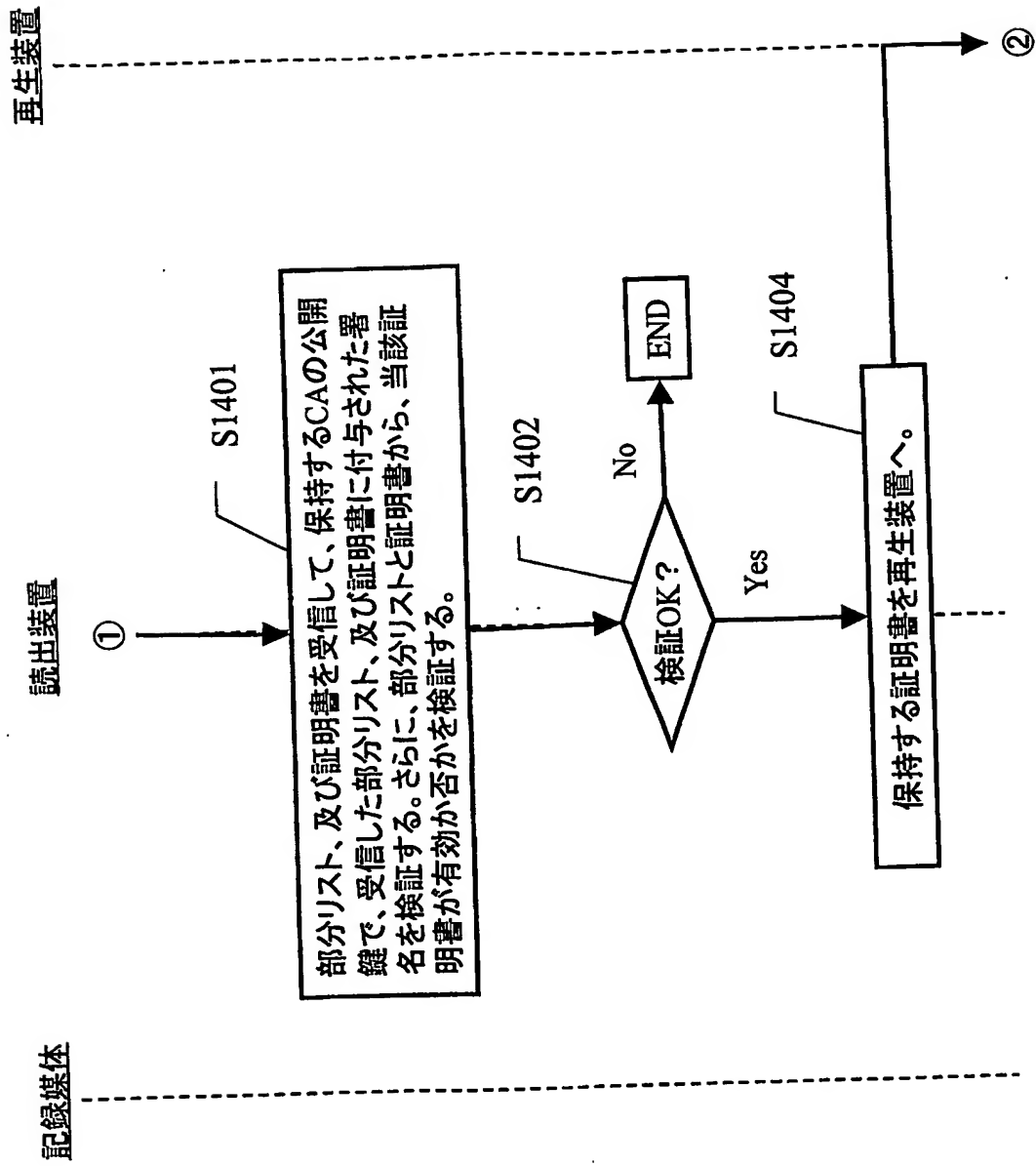
再生装置のID

x : 無効化すべきID

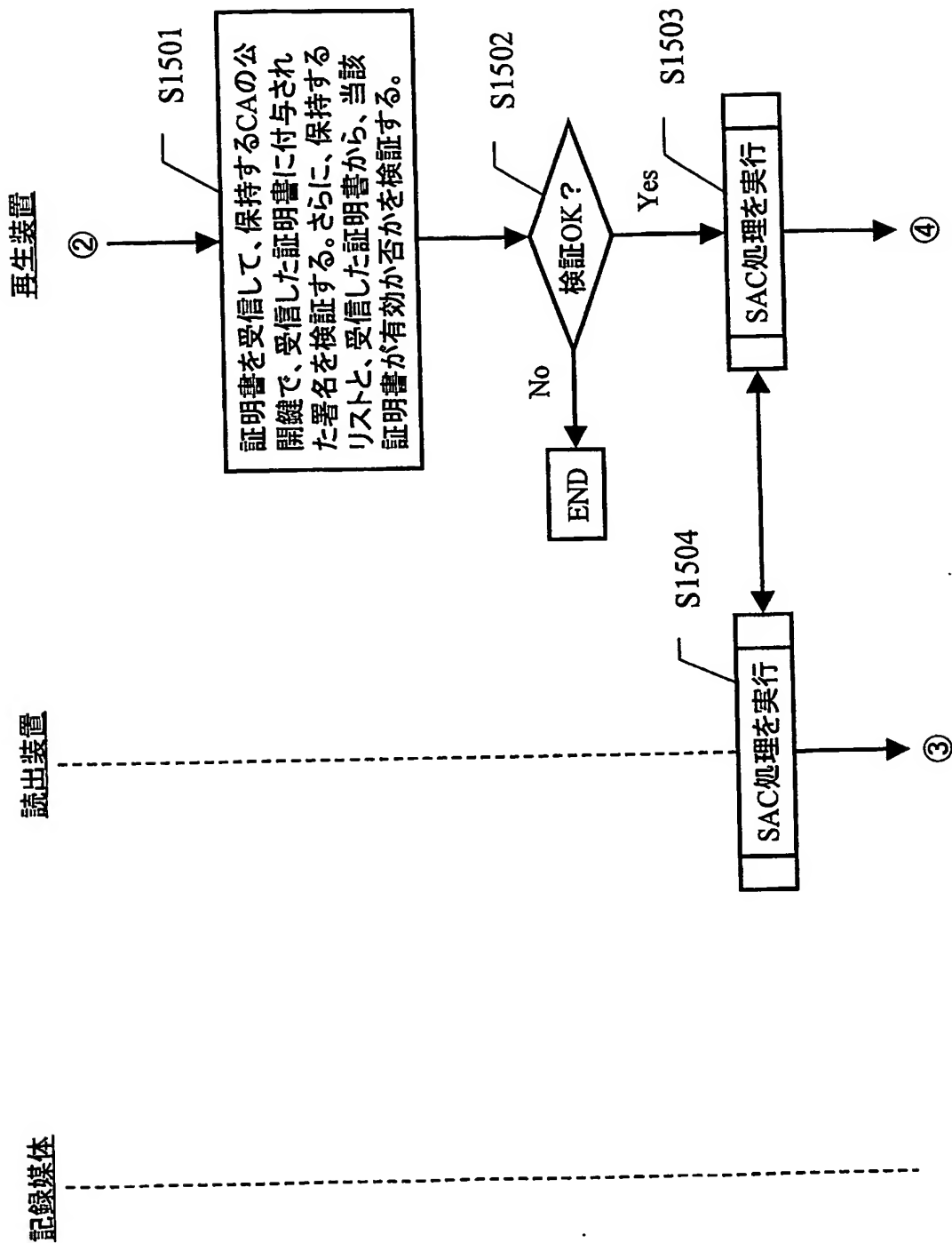
【図 13】



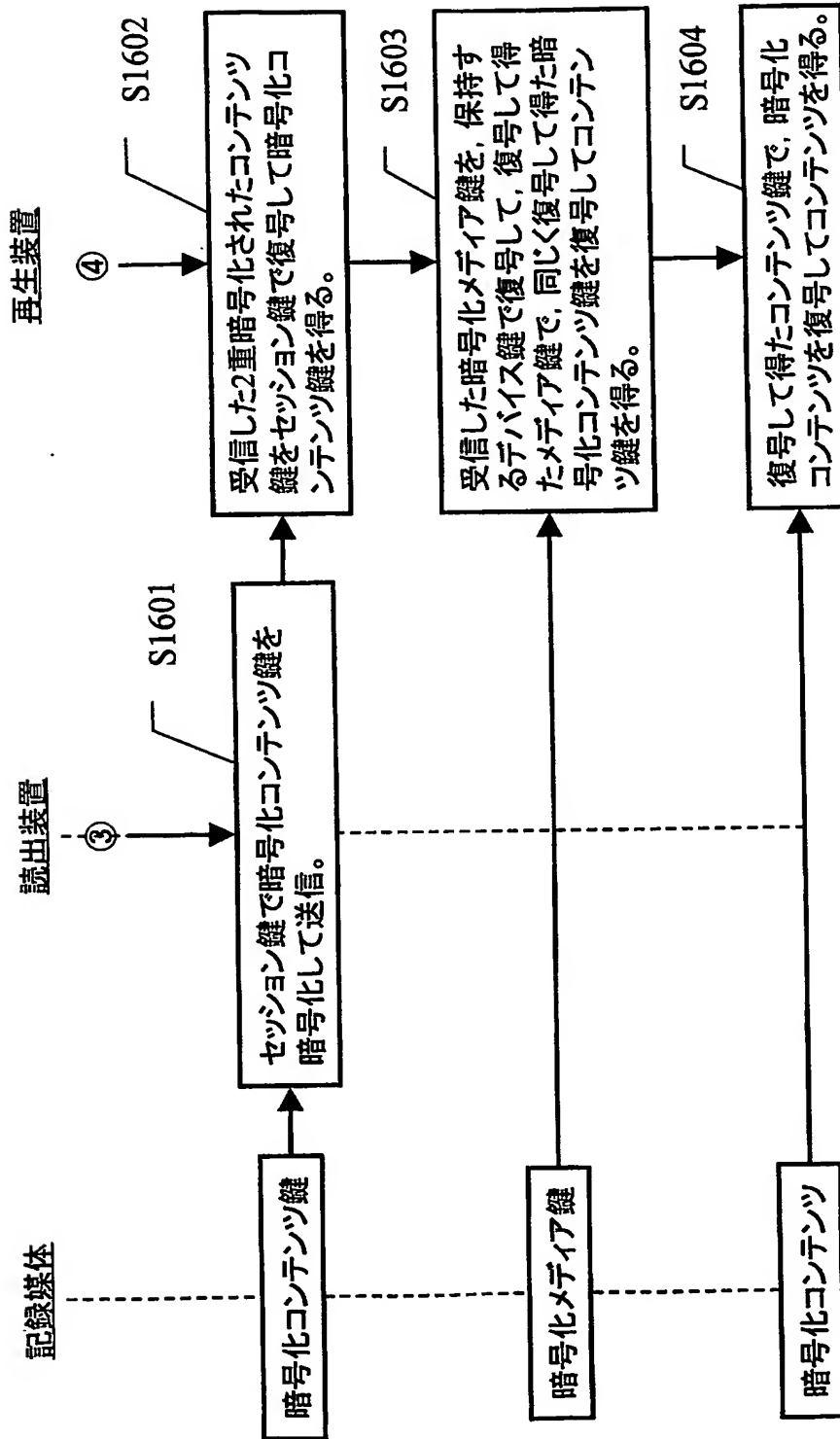
【図 14】



【図 15】



【図16】



【図 17】

バージョン番号:VN	0003	1701
無効化する証明書のID:ID1	0001	1702
無効化する証明書のID:ID2	0004	1703
有効な証明書のID:ID3	0012	1704
有効な証明書のID:ID4	0016	1705
有効な証明書の先頭ID:ID5	0018	1706
有効な証明書の終端ID:ID6	9999	1707
CAの署名	Sig1(SK_CA, Flag 0001 0008 VN ID1 ID2)	1708
CAの署名	Sig2(SK_CA, Flag 0009 0016 VN ID3 ID4)	1709
CAの署名	Sig3(SK_CA, Flag 0017 9999 VN ID5 ID6)	1710

証明書ID : x 2, 3, *, 5, 6, 7, 8, 9, 10, 14, 12, 13, 14, 15, 16, 17, 18, ..., 9999

x : 無効化すべきID

【図 18】

バージョン番号:VN	0003	1801
無効化する証明書のID:ID1	0	1802
無効化する証明書のID:ID2	0	1803
無効化する証明書のID:ID3	0	1804
無効化する証明書のID:ID4	1	1805
無効化する証明書のID:ID5	1	1806
無効化する証明書のID:ID6	0	1807
CAの署名	Sig1(SK_CA, Flag 0001 0008 VN ID1 ID2)	1808
CAの署名	Sig2 (SK_CA, Flag 0009 0016 VN ID3 ID4)	1809
CAの署名	Sig3(SK_CA, Flag 0017 9999 VN ID5 ID6)	1810

証明書ID : K 2, 3, *, 5, 6, 7, 8, 9 10, 11, 12, 13, 14, 15, 16, 17, 18, ...

x : 無効化すべきID

【書類名】 要約書

【要約】

【課題】 公開鍵暗号を利用した認証システムにおいて、通信相手が有効か無効かを判断するためだけに用いられるリストに対しては、その入手／更新に対して強制力が働かない。

【解決手段】 再生装置が、自身の有効性を通信相手に示すリストを更新するときに、通信相手が有効か無効かを判断するためのリストも合わせて更新する。あるいは、それらリストを一体化することで、前記リストの入手／更新を強制化させる。

【選択図】 図 1

特願 2 0 0 3 - 3 9 4 7 0 9

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP04/017415

International filing date: 24 November 2004 (24.11.2004)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2003-394709
Filing date: 25 November 2003 (25.11.2003)

Date of receipt at the International Bureau: 27 January 2005 (27.01.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse